

**Michigan Supreme Court
State Court Administrative Office
309 N. Washington Square, P.O. Box 30048
Lansing, Michigan 48909
(517) 373-2222 TEL
(517) 373-2112 FAX
Email Ferryj@Jud.state.mi.us
John D. Ferry, Jr., State Court Administrator**

M E M O R A N D U M:

June 13, 2000

TO: Chief Judges
cc: Court Administrators

FROM: John D. Ferry, Jr., State Court Administrator

RE: SCAO Administrative Memorandum 2000-07
Trial Court Communications Policies and Procedures

With the increased utilization of electronic means of communication, including, but not limited to, telephone and voice mail systems, e-mail (internal), internet e-mail and browsing, facsimile, etc., it has become more important than ever for local trial courts to establish policies and procedures governing internal court use of all communication devices and systems.

Often, these systems are provided through the court's funding unit. In those situations, courts need to establish, **in collaboration with the funding unit**, rules for the control (ownership) and monitoring of data generated by any systems utilized by the court. **Before providing copies of these guidelines to your funding unit, contact your Regional Administrator. He or she can assist you in facilitating the implementation of these policies.**

A. Control and Monitoring of Court Communications Systems

1. Definition

Communications Systems, include, but are not limited to:

- a. Telephone Systems
- b. Voice Mail
- c. Computer Systems, including internal e-mail
- d. Internet Connections
- e. Facsimile Equipment
- f. Interactive Video

2. Policy Requirements

When the court is provided any of its systems through its funding unit, the court should establish procedures, written in collaboration with the funding unit, for the control and monitoring of court information to assure that the information is maintained in a protected and confidential manner. Any question about access to the data and its availability to the public should be covered through these rules.

The rules or controls can be established through three alternatives or combination of alternatives: 1) joint policies and procedures agreed upon with the funding unit (see attached Model Policy for the Operation of Computer Network, Internet Access, E-Mail, Phone Service and Other Communication Equipment and Programs Utilized by the Court); 2) a contract for services between the court and the funding unit; and 3) hardware and software solutions for certain services, such as e-mail and internet access (see Section B: Computer Hardware and Software Options for Judicial E-mail and Internet Autonomy), with necessary internal operating procedures.

No matter which alternative or sets of alternatives are employed, the court should assure that the following provisions are included in any agreement, policy statement, or contract:

All data, information, or records generated in or by any Communications Systems utilized by the judges and employees of the court are the property of the court and shall not be disseminated without written approval of the Chief Judge.

Only the court will have the authority to monitor and review all data, information, or records generated by the judges and employees of the court. The Chief Judge has the sole authority to authorize appropriate action should anyone abuse the use of any system or violate any standard of operation.

The court is encouraged to adopt standards of operation that conform with those adopted by the funding unit so long as those standards do not interfere with the orderly operation of the court. If the funding unit has no standards, the court should adopt standards consistent with recommendations provided by the State Court Administrative Office (see attached Standards for Court Operations of Communication Equipment and Programs).

B. Computer Hardware and Software Options for Judicial E-Mail and Internet Autonomy

1. Introduction

Courts frequently are users of funding unit data and telecommunications systems. The advantages are obvious. Using the funding unit system offers lower cost of administration due to economy of scale and elimination of redundancy. These arrangements also make it easier to share information locally as needed for the administration of justice.

Sharing information and telecommunications systems does present challenges to the responsibility of courts to independently manage and control information for which the court has legal responsibility to fulfill its case-deciding and administrative duties.

As part of system administration, the funding unit will often impose restrictions and/or monitoring of these services on all departments, including the court. As courts begin to use e-mail as an integral means of communication, confidential correspondence will often reside on the e-mail system.

When making full use of built-in security features, internal e-mail systems are more than 99% secure. Adding internet capability to an e-mail system will reduce that security to approximately 97%. When monitoring functions are used, anyone with "system administrator" access rights will be able to read all mail, including confidential court-related correspondence. "System administrators" who are not judicial employees should not have access to court documents.

2. Policy Requirements

The following configurations provide a range of options to courts when implementing or updating court computer services.

a. Court-Only Computer Services

Courts may choose to acquire their own computer services so they are not reliant on another branch of government for services and security. This option requires adequate funding and access to competent technical support. However, courts often find it difficult to secure funding for their own computer system, especially when the funding unit has reliable, effective computer services available for the court's use.

b. Segregated Court Network

Hardware and software products are available that will permit courts to make use of funding unit-provided connectivity while maintaining control of the court computer services. With this option, courts connect to funding unit networks and implement fire walls between the court network and funding unit network. This effectively segregates court-related network traffic from the funding unit network. Courts could then implement their own e-mail gateway server, allowing judicial employees internet e-mail access over the funding unit internet connection, but limiting mail monitoring to court personnel. This option requires less funding and technical expertise than maintaining completely separate systems. Courts choosing this option should conform to existing funding unit software standards in order to minimize integration support problems.

c. Segregated Virtual Court Server

A third option is to have the funding unit e-mail server configured with two post offices, one for the court(s) and one for other funding unit departments. The court post office would then be exempted from monitoring. This option requires a high level of trust in that it would be easy for support staff to turn on monitoring of the court post office. A clear, written policy and procedure governing court and funding unit rights and responsibilities is necessary in order to maintain the principle of separation of powers. Separate backup tapes should be run on the two post offices, allowing funding units to refer requests for data to the courts. This option is the most inexpensive option. However, it may not be feasible in all cases, depending on the hardware and software in place.

C. Standards for Internal Management of Communication Systems

1. Introduction

Standards for internal management of the court's communication systems should ideally be developed for all communication media, i.e. computers, telephones, facsimile machines. The attached standards can be used as a model for internet and e-mail usage, as well as for other communication media. Every court should adopt these standards, or a similar set of standards that conforms to those established by the funding unit, so long as such standards do not interfere with the orderly operation of the court.

For help on implementation of policies and agreements with your funding unit, contact your Regional Administrator. For further technical information, contact Dan Voss at (517)373-2106.